UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/621,059	07/21/2000	Dennis K. Branstad	NAI1P079/99.122.01	4287

28875 7590 06/04/2004

SILICON VALLEY INTELLECTUAL PROPERTY GROUP
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2134	15

DATE MAILED: 06/04/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/621,059	BRANSTAD ET AL.	
	Examiner	Art Unit	
	Thomas M Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *18 March 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-8, 10-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *2,3,5,10,11 and 13* is/are allowed.

6)☒ Claim(s) *4, 6-8, 12, 14-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 2-8, 10-16 are pending.

2. The terminal disclaimer filed on 3/18/04 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of 09/621056, 09/621057, 09/621058, 09/621059, and 09/621060 has been reviewed and is accepted. The terminal disclaimer has been recorded.

3. Claims 2, 3, 5, 10, 11, 13 are allowable.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 4, 6-8, 12, 14-16 are rejected under 35 U.S.C. 102(b) as being anticipated by Bellare et al.

Claim 4 is rejected for the same reasons as claim 12.

Claim 6-8 is rejected for the same reasons as claims 14-16 respectively.

In reference to claim 12:

Bellare et al. (Section 4, NMAC) & (Section 5, HMAC) discloses a device for generating an authentication tag for a message, comprising:

- A first hashing module that processes a portion of the message to produce an interim output, where the first hashing module is the first hash function which creates an intermediate hash to be placed into the input of an outer function. (Section 5.1, The function HMAC)
- A second hashing module that processes said interim output to produce the authentication tag, where the second hashing module processes as input, the interim output. (Section 5.1, The function HMAC)
- Wherein the message is partitioned into regions, each region including a number of message parts, and one message part from each region is provided as input to said first hashing module.

In reference to claim 14:

Bellare et al. (Section 4, NMAC) & (Section 5, HMAC) discloses a device for generating an authentication tag for a message, comprising:

- A first hashing module that processes a portion of the message to produce an interim output, where the first hashing module is the first hash function which creates an intermediate hash to be placed into the input of an outer function. (Section 5.1, The function HMAC)

- A second hashing module that processes said interim output to produce the authentication tag, where the second hashing module processes as input, the interim output. (Section 5.1, The function HMAC)
- Wherein first hashing module includes a keyed hash function, where the keyed hash function is F, and one of the arguments is the key k.

In reference to claim 15:

Bellare et al. (Section 4, NMAC) & (Section 5, HMAC) discloses a device for generating an authentication tag for a message, comprising:

- A first hashing module that processes a portion of the message to produce an interim output, where the first hashing module is the first hash function which creates an intermediate hash to be placed into the input of an outer function. (Section 5.1, The function HMAC)
- A second hashing module that processes said interim output to produce the authentication tag, where the second hashing module processes as input, the interim output. (Section 5.1, The function HMAC)
- Wherein said first hashing module includes one of an MD4 hashing function, a bucket hashing function, a multilinear modular hashing function, a cyclic redundancy code-based hashing function, and an alternative hash algorithm, where the functions used include the alternative hash algorithms MD5 and SHA.

In reference to claim 16:

Bellare et al. (Section 4, NMAC) & (Section 5, HMAC) discloses a device for generating an authentication tag for a message, comprising:

- A first hashing module that processes a portion of the message to produce an interim output, where the first hashing module is the first hash function which creates an intermediate hash to be placed into the input of an outer function. (Section 5.1, The function HMAC)
- A second hashing module that processes said interim output to produce the authentication tag, where the second hashing module processes as input, the interim output. (Section 5.1, The function HMAC)
- Wherein the portion of the message processed is selected by truncating the message, wherein the authentication tag portion of the message is processed when only half of the output of the hash function is used as the authentication code. (page 12, remark 4.7)

Conclusion

6. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of the final action and the advisory action is not mailed under after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension pursuant to 37 CFR

1.136(A) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (703)305-8029. The examiner can normally be reached on M-F from 8:30am – 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (703)308-4789. The fax phone numbers for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

TMH

May 28th 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100